Secure Web 2.0 Content Sharing
Beyond Walled Gardens

San-Tsai Sun, Kirstie Hawkey, Konstantin Beznosov

Department of Electrical and Computer Engineering
Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
outline

• overview
• approach
• implementation
• conclusion
Web 2.0: user-centric Web

"Web 2.0 is a very different thing. It's a tool for bringing together the small contributions of millions of people and making them matter."


Dec. 2006

source: http://www.time.com/time/covers/0,16641,20061225,00.html
walled garden problem

lack of usable mechanisms for secure Web 2.0 user content sharing across content and service providers (CSPs)
content sharing scenario

Canadian Coast Adventures (CCA)
Girl Scouts

CCA scouts only

Alice

Jenny

Picasa Web
sharing content with unknown user
research goal

Web-based content sharing mechanism

✓ enable users to share content with unknown Web users

✓ work beyond walled gardens

investigate the applicability of existing access-control systems when apply them to realize user-centric policy in the Web
challenges

• usability - usable for average Web users

  Eric Sachs (product manager for Google security and internal systems),
  "Redirects to login pages are bad, or are they?"

  “designing hard to use security is easy
  designing easy to use security is hard”

• interoperability
  – work across CSPs boundaries
  – work under current walled garden restrictions
usability

• user-centric
  – use the same identity and access policy across CSPs

• sharing experiences should be similar to users’ existing file/content practices

• only use browser, no special software installed or crypto operations performed by user
interoperability

• build upon open standards and protocols
• for CSPs
  – provide additional content sharing channel
  – not required to change their existing access-control mechanism
existing secret-link approach

http://picasaweb.google.com/Alice?authkey=Gv1sRgCOzu

- usable for Web users
- easy to implement by CSPs
- Alice does not have control over Jenny’s sharing of secret link with others
- Alice has to know Jenny’s email

Jenny

secret-link

Picasa Web

---

jenny@aol.com

Alice
content sharing user studies

• email is the most commonly used sharing mechanism [2,3,4,5]

• users tend to treat socially-defined classes of individuals the same when sharing [1,2,3]

outline

• overview
• approach
• implementation
• conclusion
ideas

secret-link

user-centric identity provider

email

user-centric policy provider
approach

enables users to use their email to login CSPs

extends contact-lists to enable trust-based access control

OpenID provider

OpenPolicy provider

RT policy language

sharing scenario

AlicePolicy.com

CCA Policy.com

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com
access scenario

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

policy service
YahooPolicy.com

policy service
GooglePolicy.com

Alice@gmail.com.scout ← CCA.@yahoo.scout
more complex sharing scenario

CCA scouts and their parents only

Canadian Coast Adventures (CCA) Girl Scouts

Alice

Alice’s scout friends in Picasa Web

Picasa Web

Jenny @aol.com → parent
Mary @hotmail.com

CCA.scout ← Jenny @aol.com
outline

• overview
• approach
• implementation
• conclusion
implementation
RT type 1 credential statements
Selected Group: **Family**

- Siblings ✗
- Parents ✗
- Children ✗

Add group: [Add to this group]
RT type 2 credential statements
RT type 3 credential statements
RT type 4 credential statements
Edit Album - Vancouver Snow Fun 2008

Album Name: Vancouver Snow Fun 2008
Location: UBC, Vancouver
Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights.
Privacy: [Who can see this?]
- Custom
- Only Me

Save Changes  Cancel

Share this album with anyone by sending them this public link:

Transferring data from ec.atdmt.com...
Share your albums with non-Facebook users

This is research project of LERSSE in the Department of Electrical and Computer Engineering at the University of British Columbia

Tien-Lan One-Year-Old
3 photos
Tien-Lan is one-year-old now.
Created 2009/11/24
Updated 2009/11/24

UBC Apple Festival
2 photos
The 19th annual Apple Festival, hosted by the Friends of the Garden, is being held on October 17th and 18th from 11 a.m. to 4 p.m. each day. A $2.00 admission fee for adults helps support new garden initiatives -- for those under 12, admission is free.
Created 2009/11/24
Updated 2009/11/24

Vancouver Snow Fun 2008
8 photos
Tien-Lan was having great fun in building snow caves and playing snow-ball fights.
Created 2009/1/7
Updated 2009/11/24
The following link will be sent out to each member of the selected target groups:

**Facebook Photo Sharing Application**

Photo Album: **Vancouver Snow Fun 2008**
Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights.

San-Tsai Sun has shared a link to an album with you. To view the album, follow this link:
http://apps.facebook.com/fbshares/access.aspx?s=5058256540109113947
Photo Album: Vancouver Snow Fun 2008
Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights. San-Tsai has shared a link to the above album with you. To view the album, follow this link:
http://apps.facebook.com/fbshares/access.aspx?s=5058256540109113947
Sign up for Facebook to use Sharing beyond walled garden.

You do not need to sign up Facebook, just login using your existing email account.

[Google] [Yahoo!] [AOL] [Windows Live ID]
Sign in to Yahoo!

fbshares.rpxnow.com

Sign in to fbshares.rpxnow.com with your Yahoo! ID

Yahoo! ID:
santsaisun@yahoo.com
(e.g. free2rhyme@yahoo.com)

Password:

Sign In

I can't access my account
Web-based content sharing mechanism
conclusion

• our solution is user-centric
  – Web users use the same identity and access policy across CSPs, and they are free to choose them

• only use browser, sharing experiences are similar to users’ existing file/content practices
  – email, secret-link

• CSPs are not required to change their existing access-control mechanism
  – integrate their secret-link mechanism with OpenPolicy and OpenID email provider
extend OpenID

• OpenID relies on redirection during authentication  
  – vulnerable to phishing attacks
• build OpenID support into browser  
  – function without redirection


enhance trust-management

• detect who is abusing the trust of others
  – Jenny could allow her friend Bob to view CCA’s photos

• control the depth of transitive trust
  – A trusts B \( \cap \) B trusts C \( \rightarrow \) A trusts C
usability evaluation

• heuristic evaluation
• cognitive walk-through
• lab experiment
questions?

Secure Web 2.0 Content Sharing
Beyond Walled Gardens

san-tsai sun <santsais@ece.ubc.ca>

Department of Electrical and Computer Engineering
Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
sharing scenario 1

secret-link

secret-link, Alice@gmail.com .scout

policy service
YourPolicy.com

Alice@gmail.com .scout ← Betty@aol.com
Carol@hotmail.com

Picasa Web

Alice@gmail.com .scout

Alice@gmail.com .scout

Alice@gmail.com .scout
access scenario 1

Betty@aol.com

OpenID_email
AOL

Betty@aol.com,
Alice@gmail.com

yes/no

policy service
YourPolicy.com

Alice@gmail.com
.scout

Betty@aol.com

Carol@hotmail.com

secret-link

Picasa Web

Alice@gmail.com
.scout
policy import scenario

CCA

yahoo.com/CCA

OpenID_{email}

Yahoo

CCA.scout → Alice@gmail.com
CCA.scout → Jenny@aol.com
CCA.scout → Betty@hotmail.com

OpenID_{policy}

MyPolicy
construct policy scenario

Alice @gmail.com

OpenID_{email} gmail

OpenID_{policy} YourPolicy

CCA @yahoo.com

yahoo.com/CCA

mapping

Alice @gmail.com

gmail.com/Alice

Alice @gmail.com .scout

CCA @yahoo.com

gmail.com/Alice .scout

yahoo.com/CCA .scout
sharing scenario (detail)

CCA

secret-link, yahoo.com/jenny

credentials

policy service

MyPolicy

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

OpenID

email

gmail

gmail.com/Alice

yourPolicy

OpenID

email

Yahoo

secret-link,

gmail.com/Alice.scout

Picasa Web

gmail.com/Alice.scout

Alice

gmail.com/Alice.scout

Alice@gmail.com

CCA@yahoo.scout

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

policy service

YourPolicy

gmail.com/Alice

yourPolicy

OpenID

email

Yahoo

secret-link,

gmail.com/Alice.scout

Picasa Web

gmail.com/Alice.scout

Alice

gmail.com/Alice.scout

Alice@gmail.com

CCA@yahoo.scout

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

policy service

YourPolicy

gmail.com/Alice

yourPolicy

OpenID

email

Yahoo

secret-link,

gmail.com/Alice.scout

Picasa Web

gmail.com/Alice.scout

Alice

gmail.com/Alice.scout

Alice@gmail.com

CCA@yahoo.scout

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

policy service

YourPolicy

gmail.com/Alice

yourPolicy

OpenID

email

Yahoo

secret-link,

gmail.com/Alice.scout

Picasa Web

gmail.com/Alice.scout

Alice

gmail.com/Alice.scout

Alice@gmail.com

CCA@yahoo.scout

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

policy service

YourPolicy
access scenario

Jenny @aol.com

CCA

Alice @gmail.com

Jenny @aol.com

Betty @hotmail.com

gmail.com/Alice

OpenID_email

aol.com/Jenny

secret-link

OpenID_email

yourPolicy

gmail.com/Alice

Picasa Web

gmail.com/Alice .scout

yes/no

aol.com/Jenny, gmail.com/Alice .scout

policy service

MyPolicy

credentials

policy service

YourPolicy

Alice @gmail.com .scout

CCA .yahoo .scout

CCA .scout

CCA .scout

CCA .scout